Testimony of David W. Aucsmith,
Chief Security Architect, Intel Corporation
Before Senator Jon Kyl, Chairman of the
Subcommittee on Technology, Terrorism, and Government Information of the
Senate Judiciary Committee
April 21, 2000

Thank you Senator Kyl for the opportunity to testify on the important topic of cyber security. My name is David Aucsmith, and I serve as Chief Security Architect for Intel Corporation. In this capacity, I am responsible for data and communications security in Intel products and services. I also serve as the technical liaison to the law enforcement and intelligence communities, My background prior to joining Intel includes over twenty years of service in both the government and private sector in the fields of information security and cryptography.

At the outset, let me say a few words about Intel. Intel is the world's largest semiconductor manufacturer and a leading producer of computer, networking and communications building blacks to the Internet economy. Intel's flagship business continues to be the mass production and sale of the Pentium7 processor family and other microprocessors. At the same time, our business is expanding beyond supplying the PC industry with chips and related printed circuit boards to providing Internet solutions in such areas as wireless products, networks and communications, and on-line services. In 1999, our sales exceeded $29 billion.

Cyber security plays a major role in the conduct and growth of Intel's business. The ability to safeguard networks and information systems on a global basis is increasingly critical to internal company operations, intellectual property protection, e-business, and on-line services. This trend is graphically illustrated by Intel's e-commerce activities, which have skyrocketed from zero to $1 billion in monthly sales over the last few years. In addition, user requirements for on-line security have led Intel to pursue security as a commodity feature of information technology (IT) products, an endeavor greatly facilitated by the Administration's recent encryption policy reforms. For example, in May, we will make source code for strong Intel security software freely available on the Internet, increasing industry capability to build IT products with security management capabilities.

The importance of cyber security is especially relevant to critical infrastructures upon which companies like Intel must rely. As with the public, Intel relies heavily on stable telecommunications, Transportation energy, water, banking and other infrastructures. These infrastructures are largely and increasingly dependent on networks and information systems it is therefore in Intel's vested interest to help prevent destabilizing cyber attacks on critical infrastructures to the greatest extent possible.

Today, my testimony will reflect Intel's strong dedication to cyber security by addressing three areas applicable to any consideration of security threats and countermeasures:

- IT industry trends in addressing cyber security challenges

$ The role of industry and government in addressing threats to cyber security

$ Recommended course of action

I. IT Industry Trends in Addressing Cyber Security Challenges

A. Need for a Secure Information Infrastructure

Today's global information infrastructure is characterized by more than 95 million network-connected computers, most of which are located in open environments with little or no physical control. This infrastructure cuts across all other critical infrastructures. Indeed, interconnected computers are used to control defense facilities, energy grids, financial institutions, the telephone system, industry and government networks, e-commerce and much more. The global information infrastructure has essentially become permanently interwoven into the fabric of our daily lives.

The following statistics, based on the American Electronic Association's recent report entitled Cybernation 2.0, illustrate the ever-increasing pervasiveness of the information infrastructure throughout the world:

Computers in Use by Regional Groupings (in thousands)

REGION	1993	2000	Percent Change 1993-2000
North America	83,391	182,600	119%
EU	44,283	134,559	204%
European Free Trade Ass-n	1,888	6,157	226%
Central & Eastern Europe	2,169	11,913	449%
Asia-Pacific	24,972	115,581	363%
Latin America	3,121	17,963	476%
Other	11,528	60,910	428%
World Total	171,352	529,683	209%

Source: Computer Industry Almanac, Inc.

Internet Users by Regional Groupings (in thousands)

REGION	1998	2000	Percent Change 1998-2000
North America	83,656	148,980	78%
EU	31,296	79,282	153%

European Free Trade Ass-n	2,434	4,774	96%
Central & Eastern Europe	1,667	4,699	180%
Asia-Pacific	21,466	50,512	135%
Latin America	1,742	7,194	313%
Other	7,143	20,407	186%
World Total	149,404	315,848	111%

Source: Computer Industry Almanac, Inc.

The rise of the global information infrastructure is having enormously positive transformational effects on society. It is creating scale economics and expanded information-based capabilities that are improving commerce, business, education, health care, defense, the media and many other sectors. The impact of this transformation has been so profound that many now talk in terms of the "Internet" or "new" economy versus the "old" economy.

The viability of the networked world is dependent on user trust and confidence in networks and associated information systems. Along with privacy, cyber security is a key enabler of user trust and confidence. It is required to safeguard the storage and transmission of data against malicious hackers, and others that engage in activities ranging from credit card fraud to stealing trade secrets to disrupting the operation of critical infrastructures.

It is thus in industry's self-interest to promote cyber security measures to the maximum extent possible, taking into account the need for corporate and personal privacy. What are the industry trends and challenges in this vital area? The question requires answers in several contexts, including security technologies/products, security standards, best practices, and information-sharing on cyber threats.

Security Technologies/Products. Presently, global networks use a wide variety of software and hardware with no common security policy. While some hardware and software security products have been available on a mass-market basis, security products have not generally been cost effective, typically filling only niche markets. Furthermore, the lack of integration and interoperability of security tools with other network management tools means that security produces cannot be -successfully incorporated into modem remote support strategies. Most companies leave security management and monitoring plans on the shelf for just this reason.

Meanwhile, both the value and volume of on-line information has sharply risen. This includes organizational information such as financial data, manufacturing information, customer information, medical and legal records, and human resources data. Additionally, there is a growing amount of data which has intrinsic value, such as monetary instruments (e.g., credit cards, coupons, etc.) and intellectual property (e.g., movies, images, etc.).

The availability of on-line security services and security products like intrusion detection, anti-virus and encryption software is nevertheless growing. Ultimately, the inexorable need for secure networks and systems is likely to make security a commodity feature of IT products and information services. But integration and interoperability challenges must be overcome to successfully enable security

implementations at the organizational level.

Security Standards. Today, communications security is being addressed by IP/SEC (Internet Protocol Security), SSL (Secure Sockets Layer) and authentication methodologies that employ smart cards and biometric. EP/SEC. which protects Internet data, has been under development over the last 5 years within a body known as the Internet Engineering Task Force. Some 50 vendors now supply IP/SEC-compliant products. Meanwhile, SSL has become a widely accepted standard for e-commerce and is typically represented by a lock on browsers. As for authentication methodologies, international consortia are now working on the interoperability of smart cards to ensure high resistance to attacks. The effort includes work on standardizing biometric, such as fingerprint and face recognition.

While the above standards are applicable to e-commerce, they are finding their way into other applications as well. For example, the military is using smart cards for ID purposes.

The key to quick, and broad implementation of security solution is fast turn-around in the standards-setting process. Uniform standards are needed to promote integration and interoperability of security products with existing infrastructures. Today, standard-setting is an international process driven by divergent market and political forces. The process is therefore ad hoc, slow and unpredictable by nature.

Best Practices. Recent cyber attacks have precipitated considerable discussion over the need for workable security practices by government and the private sector. Increasingly, there is recognition that users must deploy authentication. encryption, firewalls or other technologies as well as smarter on-line behaviors to thwart cyber attacks. To the extent users are educated on best security practices, they will be able to deploy countermeasures that reduce threats and vulnerabilities.

However, network attacks cannot be totally prevented. Hackers will always find software or system flaws to exploit. Thus, security products and best practices may well have to be supplemented by security services that provide continually updated and real-time detection and response capability. The problem is akin to an arms race in which one side must always update technological capabilities and behavioral patterns to keep ahead of the other side.

Information Sharing. The White House publication "National Plan for Information Systems" makes it clear that all cyber security stakeholders must coordinate together to counter threats and vulnerabilities. Such coordination is already underway. In recent months, the broad-based Partnership for Critical Infrastructure Security was established to help provide solutions to infrastructure security problems. The partnership consists of representatives of many companies, trade associations and federal departments and agencies.

Sharing of knowledge among partnership stakeholders is a key priority for dealing with information attacks and vulnerabilities. Under the auspices of the Information Technology Association of America, many companies from the information and communications sectors are already working to establish a mechanism for the systematic and protected coordination of information regarding cyber attacks, vulnerabilities, countermeasures and best practices. This should provide an effective early warning system over time, provide that antitrust or other barriers to information sharing can be overcome.

B. Technological Trends and Law Enforcement

The very technologies that empower computers, networks and security capabilities have a direct impact on law enforcement's ability to access plaintext communications or stored data. These technologies are a function of strong forces for technological innovation. The same innovation that has brought the richness

and efficiency of the connected world has also brought challenges to the "old" ways of conducting business - including the business of law enforcement.

Digitalization

Clearly the most dramatic trend is the movement from analogue to digital representations of information. Any information can and will be represented in digital form. Digital information can be stored and transmitted with no loss of content or fidelity. It can he easily manipulated and replicated. The ease in manipulation means that information can be easily transformed into representations that are difficult to detect or understand unless complete knowledge of the transformation is available. Digital voice, for examples is indistinguishable from digital stock quotes if the transformation and protocol are unknown. In the end, "bits are just bits."

Cryptography

Only cryptographic technologies are capable of projecting Security onto the completely open, arbitrary environment that is the Internet. Cryptography, by itself, does not guarantee any level of security. It is a necessary component but not a sufficient component. It can provide the essential component of authentication, confidentiality, and integrity. It can guard intellectual property and ensure that a banking transaction is not 1rauduleyit. It can also shield child pornography and keep a drug deal secret. Overall, there are significant forces propelling the wide use of cryptographic technology such as the IP/SEC standard and the Advanced Encryption Standard from NIST.

Digital Modem Protocols

Computational bandwidth is increasing at a substantially greater rate than communications bandwidth. This inequality favors trading off more strenuous computation for more effective communications bandwidth utilization. There are several technologies currently under development to maximize communications channel utilization that will pose serious barriers to communications intercept.

Data Specific Compression Algorithms

Many data-specific communications protocols, such as the H.323 video conferencing protocol, contain data specific compression algorithms (e.g., MPEG) which, without knowledge of the type of data being exchanged, resemble encryption at the point of intercept. Again, in order to maximize communications bandwidth, the trend is toward the development of data-specific compression that effectively renders data communications intercept unreadable.

Multiple Communications Paths

One way of overcoming communications channel bandwidth constraints is to utilize multiple communications channels. There are many commercial developments underway to use nontraditional communications channels for data communications, such as cable TV, satellite broadcast, and the electrical distribution system. Interception of communications at the "common carrier" may require access to many different communications infrastructures. Interception will be made even more difficult when the individual packets of a given communications session re dispersed among a wide range of infrastructures.

Steganography

There has been active academic research into stenographic communications protocols. These protocols pose perhaps a greater barrier to interception of plain-text communications than does cryptography. By their design, they prevent an eavesdropper from being able to detect the very existence of information being communicated between two or more parties.

Voice Over IP

Perhaps the most significant technological trend confronting law enforcement is the move toward voice communications over the Internet. This will render most of the established voice interception methods

ineffective and will allow all of the other technical trends to apply to normal voice communication such as encryption, compression, multiple communications paths and steganography.

New challenges. The challenge for law enforcement is to adapt to changing technology and find, within it, the means to perform their job. This is not the first time that this has happened. Throughout history, law enforcement has needed to adapt to new technology. It adapted to both the automobile and the telephone over time. The difference today, with the Internet and computers, is merely in the degree of complexity of the technology and the speed of implementation.

Once the technology and its evolution am understood, there is opportunities for both lawful interception and seizure of evidence. The problem faced by law enforcement is not one of unsympathetic technology but, rather, a lack of expertise and resources.

Technological Solutions. Dealing with technological change is a daunting task - even for those immersed in its day-to-day creation. This is especially true for law enforcement because:

- The technology changes more rapidly than any published information about it
- The general direction of technology can only be comprehended with a visibility into many diverse industry standards activities
- The complexity of much of the technology is only comprehendible to experts
- Technology experts are in great demand and frequently command financial compensation well above that which could be offered by law enforcement organizations
- Mandating technology solutions to solve law enforcement problems relative to information technology does not work (for reasons explained later in this testimony).

Clearly the only solution that makes sense is for those who create technology to team up with those who must use that technology to enforce the law. There must be a continued information flow from industry to the government if there is to be a viable option for achieving lawful access to plaintext data. Such an arrangement already exists informally by way of a joint industry / FBI cooperative effort known as the Information Technology Study Group. All that is left is for congress to adequately fund a technical support center that formalizes this arrangement.

II. Role of Industry and Government in Addressing Cyber Security Threats

A. Cyber Security Efforts Should Be Industry-Led

As recent Internet viruses and denial of service attacks have reminded us, more need to done to secure the information systems that many sectors of the U.S. economy (utilities, banking, communications, transportation, health care, e-commerce) as well as the U.S. government rely upon extensively. Protecting the information infrastructure used for these critical sectors is essential to U.S. national security, American economic welfare, and our fundamental freedoms.

Intel believes that critical information infrastructure protection (CIIP) is best accomplished through private sector solutions that are market driven and industry led. The private sector not only builds and maintains the products, networks, and systems that make up the information infrastructure but also possesses the

knowledge and expertise necessary to protect it.

As noted earlier, it is in industry's self-interest to protect the networks and information systems that form the backbone of critical infrastructures. For instance, safeguarding the privacy and security of every member of the Internet community is top priority at Intel. Such protection is essential to the future growth of the Internet and e-business. Without it, user trust and confidence in "the networked world" will wane, jeopardizing the economic health of IT companies.

B. Government Should Play a Supportive Role

Intel believes the U.S. Government should support industry efforts to secure information-based infrastructures. Government support should include facilitating industry sharing of knowledge on cyber threats, vulnerabilities and countermeasures. It should entail measures to protect the privacy and security of government computer systems and networks using industry best practices. It should include sharing results of government-funded cyber security research with industry and encourage academic research. Finally, it should involve punishment of cyber crimes by aggressively enforcing criminal and civil laws.

Importantly, the U.S. government has so far recognized that it should work cooperatively with industry on a voluntary basis to deter, identify and respond to cyber threats and attacks. The Administration has also proposed -- and Congress has funded -- numerous initiatives to strengthen the government's technological capabilities.

C. Government Policies Must be Workable

Intel applauds the Administration's current cyber security initiatives and will cooperate with the government in their implementation. However, Intel is concerned about possible overreaction to denial-of-service or other potential cyber attacks. Such overreaction could generate new laws or regulations that would stifle innovation, artificially channel R&D, and harm the very infrastructure that needs protection.

It is essential that the government not use legitimate threats to cyber security as a justification for assuming broad new powers of regulation, imposing new burdens upon industry, or threatening fundamental rights of privacy. As a matter of practice, the government should only pass new laws or adopt new regulations where it is demonstrated that current legal regimes are inadequate. Any new legal requirements, however, should not mandate information tracking, access requirements or other capabilities/standards for IT technologies. The government must also not engage in broad surveillance or networks and information systems. There are several reasons for these caveats:

$ <u>Technology mandates are technologically unworkable in the IT industry.</u> The IT industry is characterized by an open, international horizontal architecture that makes one-size-fit all solutions (like built-in access capability) technologically unworkable. Unlike the centralized telecom infrastructure, there is no "top-down" control of information technology products and related networks. Further, uniform adoption of special product protocols in IT environment is extremely difficult because standards-setting is largely ad

hoc, decentralized and global. Thus, by definition, technology mandates cannot succeed because there is no binding mechanism to ensure that all IT architectural layers (from components to computer platforms cooperating systems to network protocols) will comply with government requirements.

(NOTE: Rapid technological advances compound the problem. Assuming the government chose to mandate technological requirements. advances in technology would soon outpace the scope of those requirements, creating the need for new regulations on a continuous basis. This would spawn an unworkable regulatory treadmill.)

$ Global IT standards are highly likely to embrace mandated tracking or access capabilities in any case. Government-mandated tracking or access capabilities create information vulnerabilities that threaten IT security and consumer privacy. Global marketplace acceptance of products and commercial infrastructure featuring such capabilities is therefore very unlikely. Absent market acceptance, there will be no impetus for adoption of enabling technology standards. One standards body, the Internet Engineering Task Force, has already rejected imposition of CALEA (Communications Assistance for Law Enforcement Access) standards for the Internet.

$ Broad on-line surveillance will undermine trust and confidence in the Internet. the economic backbone of the IT industry. If users perceive that security and privacy on the Internet are being compromised by broad government surveillance activities, they will likely choose to avoid this medium. This could have profoundly negative economic consequences for the IT industry and the Internet economy as a whole, since innovation and development of IT products is now largely driven by Internet growth.

III. Recommended Course of Action

Intel believes efforts to address cyber security threats, vulnerabilities and countermeasures should rest on a firm set of principles. In particular, we endorse the principles adopted by Americans for Computer Privacy (ACP) to guide government decision-makers. ACP is a broad-based coalition that brings together more than 100 companies and 40 associations representing financial services, manufacturing, telecommunications, high-tech and transportation, as well as law enforcement, civil-liberty, pro-family and taxpayer groups. The ACP principles are as follows:

1. CIIP is best accomplished through private sector solutions that are market driven and industry led;
2. Governments and industry must work cooperatively on a voluntary basis towards achieving CIIP;
3. Government must not mandate the choice of technologies or dictate standards or processes
4. Govemment must not violate personal and corporate privacy in the quest for CIIP; and
5. Barriers to strong CIIP should be removed, including barriers to the widespread use of strong encryption.

Based on these principles, Intel believes that the model for undertaking CIIP efforts should include the following elements:

RESPONSIBILITY	ACTION

IT Industry	Develop best cyber security practices
IT Industry/Academia/Government	Educate public on risks and safeguards
IT Industry	Develop and deliver security technologies/tools
IT Industry/Academia	Perform R&D to address threats and develop solutions
IT Industry	Establish knowledge-sharing mechanism within industry to address threats, vulnerabilities and countermeasures. Enlist support from government and academia.
Government	Remove antitrust or other barriers industry knowledge-sharing.
Government/Industry	Provide scholarships to increase America-s security workforce and related expertise.
Government	Provide appropriations to safeguard government networks B i.e., make sure the government-s Ahouse@ is in order.
Government	Provide appropriations for government-sponsored R&D that can be shared with private Industry
Industry	Share expertise with government to address crime in a digital world.
Government	Fund a technical support center to carry out the above sharing of expertise on a systematic basis.
Individuals, Consumers, Businesses	Increase security expertise; use best practices, tools and services provided by the IT industry.

This model, while illustrative rather than comprehensive, is an attempt to recognize the recurrent and evolving nature of cyber threats. Accordingly, it establishes remedies that systematically address problems over time.

We urge you to consider the merits of this approach as you continue your efforts to address the cyber security issues.

Thank you, Senator Kyl, for the opportunity to testify at this important hearing today, I will be glad to respond to any questions that you rnay have.